J M S K
Jurnal Matematika, Statistika, & Komputasi
http://journal.unhas.ac.id/index.php/jmsk
Vol. 9, No.2, 86-94, Januari 2013
ISBN:1858-1382

Dari Simbol Legendre ke Simbol Residu Kubik

Loeky Haryanto[1] dan Arman Efendi[2]

Abstrak

Konsep simbol Legendre yang nilainya pada setiap bilangan bulat bukan kelipatan p sama dengan akar dari $x^2 = 1$, yaitu ±1, diperluas ke konsep simbol residu kubik yang nilainya merupakan akar-akar dari $x^3 = 1$. Dengan memilih akar kompleks $\omega = e^{2\pi i/3}$, akar primitif ketiga dari 1, diturunkan lapangan siklotomik **Q(ω)** yang merupakan *splitting field* dari polinom primitif $p(x) = x^2 + x + 1$. Subgelanggang

$$\mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\} \subseteq \mathbf{Q}(\omega)$$

apabila dilengkapi norma δ: $\mathbf{Z}[\omega] \to \mathbf{N}$ dengan $(\alpha) = \alpha\bar{\alpha}$ membentuk daerah Euclid. Dari unsur prima $\pi \in \mathbf{Z}[\omega]$ terbentuk lapangan $\mathbf{Z}[\omega]/<\pi>$ dan residu kubik $\left(\frac{\alpha}{\pi}\right)_3$, di mana $\alpha \in \mathbf{Z}[\omega]$ bukan kelipatan dari π .

Kata Kunci: *Akar primitif ke*-3 *dari* 1, *simbol Legendre, lapangan siklotomik, simbol residu kubik.*

Abstract

The value of Legendre symbol at any integer, which is not a multiple of a prime p,is a root of the quadratic equation $x^2 = 1$, i.e. ±1. The Legendre symbol is generalized to cubic residue symbol having valuesamong the roots of the cubic $x^3 = 1$. By choosing complex numberω = $e^{2\pi i/3}$, the 3^{rd} promitive root of 1, the cyclotomic field**Q(ω)**, whichthe splitting fieldof primitive polinom$p(x) = x^2 + x + 1$, is derived. The subring

$$\mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\} \subseteq \mathbf{Q}(\omega)$$

equipped with Euclidean normδ: $\mathbf{Z}[\omega] \to \mathbf{N}$ where $(\alpha) = \alpha\bar{\alpha}$, forms an Euclidean domain. Every prime element$\pi \in \mathbf{Z}[\omega]$ determines a field$\mathbf{Z}[\omega]/<\pi>$and cubic residue $\left(\frac{\alpha}{\pi}\right)_3$, where$\alpha \in \mathbf{Z}[\omega]$is not a multiple of π .

Keywords: Third primitive root of 1, Legendre symbol, cyclotomic field,cubicresidue symbol.

1. Pendahuluan

Dalam komunikasi data secara digital, semua data pada umumnya dikonversi menjadi bilangan, sebagian besar dalam basis 2 (bilangan biner). Dengan demikian konsep teori bilangan, termasuk yang dibahas secara aljabar (*algebraic number theory*), sangat berpotensi sebagai

[1]*Jurusan Matematika FMIPA Universitas Hasanuddin, email: haryanto@unhas.ac.id*
[2]*Mahasiswa S2 Program Studi Matematika FMIPA Universitas Hasanuddin, email: armanefendi@gmail.com*

mathematical tool yang sangat ampuh di dalam pemodelan dan perancangan sistem yang dibuat untuk meningkatkan keamanan data komunikasi, termasuk perancangan sistem kriptografi.

Beberapa skema kriptografi publik memiliki tingkat keamanan yang bisa dihitung (*provably secure*). Salah satu skema kriptografi yang *provably secure* adalah skema kriptografi yang menggunakan lapangan siklotomik. Implementasi lapangan siklotomik pada kriptografi yang diketahui sudah ada saat ini hanya lapangan siklotomik ke-2 dan ke-3, masing-masing berbasis pada akar primitif ke-2 dan ke-3 dari 1.

Implementasi lapangan siklotomik ke-2 dan ke-3 sangat erat berkaitan dengan konsep simbol Legendre dan simbol residu kubik yang dikenal luas dalam teori bilangan. Tulisan ini merupakan hasil studi literatur sebagian teori yang menjadi dasar penerapan konsep lapangan siklotomik dalam kriptografi.

2. Algoritma Pembagian Euclid

Algoritma pembagian Euclid di antara bilangan-bilangan bulat telah dikenal secara luas. Algoritma ini berbasis dua teorema berikut.

Teorema 1.
Untuk setiap bilangan bulat positif a dan bilangan bulat b, terdapat bilangan bulat q dan bilangan bulat r yang memenuhi:

1. $a = qb + r$, *dan*
2. $0 \le r < |b|$.

Generalisasi dari gelangang bilangan bulat adalah sebuah gelanggang **G** yang disebut daerah Euclid. Sesuai dengan namanya, di dalam daerah Euclid, algoritma pembagian Euclid berlaku, di mana peran $|b|$ digantikan oleh sebuah fungsi $\mathbf{G} \rightarrow \mathbf{Z}_{\ge 0}$ yang disebut **norma** atau **fungsi Euclid**.

Manfaat utama dari algoritma pembagian Euclid dalam **Z** adalah untuk mencari FPB (faktor persekutuan terbesar) dua bilangan bulat a dan b: FPB(a, b). Berdasarkan definisi, FPB(a, b) tak pernah negatif. Sebagai akibatnya

$$\text{FPB}(a, b) = \text{FPB}(-a, b) = \text{FPB}(a, -b) = \text{FPB}(-a, -b)$$

sehingga penerapan algoritma Euclid bisa dibatasi hanya pada dua bilangan positif a dan b.

Teorema 2.
Untuk setiap pasang bilangan bulat positif a dan b berlaku:

$$\text{FPB}(a, b) = \text{FPB}(b, a \bmod b).$$

Jika dipilih $a > b > 0$, teorema kedua ini membuka jalan bagi algoritma Euclid untuk membuat daftar sisa hasil bagi

$$r_0 = a > r_1 = b,\ r_2 = a \bmod b > \ldots,\ r_n > r_{n+1} = 0$$

di mana $r_{k-1} = qr_k + r_{k+1}$, dan menyimpulkan bahwa

$$\text{FPB}(a, b) = \text{FPB}(r_0, r_1) = \text{FPB}(r_1, r_2) = \ldots = \text{FPB}(r_{n-1}, r_n) = \text{FPB}(r_n, 0) = r_n.$$

Algoritma Euclid bisa diperluas untuk memenuhi hasil teorema berikut.

Teorema 3.

Untuk setiap pasang bilangan bulat positif a dan b, terdapat dua bilangan bulat s dan t sedemikian sehingga

$$\text{FPB}(a, b) = sa + tb.$$

Algoritma Pembagian Euclid (Yang Diperluas).

INPUT: Bilangan bulat positif a, b; keduanya tidak sama dengan 0.

1. $q := \lfloor a/b \rfloor$;
2. $u_1 := a$; $u_2 := 0$; $u_3 := 1$; $u_4 := 0$ (definisi awal **U** = (a, 0, 1, 0))
3. Jika $0 < b \leq a$, makacetak **U** = (u_1, u_2, u_3, u_4)
4. $v_1 := b$; $v_2 := q$; $v_3 := 0$; $v_4 := 1$ (definisi awal **V**= (b, q, 0, 1))
5. Cetak **V**= (v_1, v_2, v_3, v_4);
6. while (u_1 mod $v_1 > 0$) do
   6.1 $w_1 := u_1 \bmod v_1$; $w_2 := \lfloor v_1/w_1 \rfloor$; $w_3 := u_3 - v_2 v_3$; $w_4 := u_4 - v_2 v_4$; (definisi **W**)
   6.2. $q := w_2$;
   6.3. **U**:= **V**; **V**:= **W**; (*update***U**,**V** dan **W**)
   6.4. Jika $0 < b \leq a$.cetak v_1, v_2, v_3, v_4;
   end (mengakhiri *loop*)

OUTPUT: v_1, v_3, v_4
Keterangan: $v_1 = \text{FPB}(a, b) = v_3 a + v_4 b$, $v_3 = s$, $v_4 = t$.

Contoh.
Algoritma pembagian Euclid yang diperluas untuk kasus-kasus a dan b, misalnya a = 469, b = 203berukuran kecil sangat mudah digambarkan melalui skema berikut.

Tabel 1. Ilustrasi Algoritma Euclid Yang Diperluas
(Untuk a = 469 dan b = 203).

k	r_k	q_k	s_k	t_k
0	469	0	1	0
1	203	2	0	1
2	63	3	1	–2
3	14	4	–3	7
4	7	2	13	–30
5	0		–29	67

Di dalam algoritma, setiap langkah dari loop memperlakukan 3 baris berurutan dalam skema di atas sebagai baris **U**, **V** dan **W**. Dalam contoh ini, output dari algoritma di atas adalah $v_1 = 7$, $v_3 = 13$ dan $v_4 = -30$. Ini berarti $7 = \text{FPB}(469, 203) = (13)(469) + (-30)(203)$.

Sesungguhnya algoritma Euclid di **Z** di atas bisa diperluas dan diberlakukan pada setiap daerah Euclid selain **Z** untuk menentukan FPB dua unsur atau invers suatu unsur modulo suatu unsur lain yang relatif prima terhadap unsur tersebut.

3. Residu Kuadratis

Simbol Legendre $\left(\frac{a}{p}\right)$ dengan a, $p \in \mathbf{Z}$, p prima dan a bukan kelipatan p**,** didefinisikan atas dasar konsep kongruensi modulo suatu bilangan prima dan fakta bahwa untuk setiap bilangan prima p,grup perkalian

$$\mathbf{Z}^{\times}_{p} = \{x \in \mathbf{Z} \mid 0 < x < p, \text{FPB}(x, p) = 1\}$$
$$= \{1, 2, ..., p - 1\}$$

terpartisi dua sama besar atas:

i. unsur-unsur $r \in \mathbf{Z}^{\times}_{p}$ dengan sifat: kongruensi $x^2 \equiv r \bmod p$ memiliki solusi; dan
ii. unsur-unsur $s \in \mathbf{Z}^{\times}_{p}$dengan sifat: kongruensi $x^2 \equiv s \bmod p$ tidakmemiliki solusi.

Sebagai akibat dari partisi $\mathbf{Z}^{\times}_{p} = \{r\} \cup \{s\}$, subhimpunan semua bilangan bulat yang bukan kelipatan p, yaitu

$$\mathbf{Z} - \langle p \rangle$$

juga terbagi dua:

i. unsur-unsur $a \in \mathbf{Z} - \langle p \rangle$dengan sifat $a \equiv r \bmod p$, yaitu unsur-unsur a yang bukan kelipatan p tetapi kongruensi $x^2 \equiv a \bmod p$ memiliki solusi. Dalam hal ini didefinisikan $\left(\frac{a}{p}\right) = 1$ dan a disebut **unsur residu kuadratis modulo *p***;

ii. unsur-unsur $a \in \mathbf{Z} - \langle p \rangle$dengan sifat $a \equiv r \bmod p$, yaitu unsur-unsur a yang bukan kelipatan p dan kongruensi $x^2 \equiv a \bmod p$ tidak memiliki solusi. Dalam hal ini didefinisikan $\left(\frac{a}{p}\right) = -1$ dan a disebut **unsur nonresidu kuadratis modulo *p***;

Bisa dibuktikan, untuk setiap bilangan bulat $a \in \mathbf{Z} - \langle p \rangle$berlaku

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p.$$

Setiap bilangan bulat a yang merupakan kelipatan p tidak termasuk ke dalam salah satu di antara bilangan residu atau nonresidu modulo p. Dalam hal ini didefinisikan $\left(\frac{a}{p}\right) = 0$, walaupun nilai simbol Legendre 0 tidak pernah dilibatkan lagi dalam pengembangan teori residu kuadratis lanjutannya.

Konsep simbol Legendre dipergunakan sebagai basis pendefinisian konsep simbol Jacobi $\left(\frac{a}{b}\right)$ yang meniadakan syarat prima untuk bilangan b. Misalkan$b$adalah bilangan positif dan ganjil yang faktorisasinya atas bilangan-bilangan prima adalah

$$b = q_1, q_2, ..., q_k$$

dengan $q_1\ q_2 \ldots\ q_k$prima, tidak harus berbeda satu sama lain. Untuk setiap bilangan bulat a dan b yang saling relatif prima,simbol Jacobididefinisikan sebagai

$$\left(\frac{a}{b}\right) = \prod_{j=1}^{k} \left(\frac{a}{q_j}\right).$$

Jika *b* prima, simbol Jacobi adalah juga (sama dengan) simbol Legendre.

4. Lapangan Siklotomik ke-*n*

Sebuah bilangan ω disebut **akar primitif** ke-*n* dari 1 jika $\omega^n = 1$ tetapi untuk setiap $k \in \{1, 2, ..., n-1\}$ berlaku $\omega^k \neq 1$. Akar primitif ke-2 dari 1 adalah −1, sebuah bilangan real dan akar primitif −1 ini bersama bilangan 1 digunakan dalam definisi residu kuadratis (simbol Legendre dan simbol Jacobi). Akar primitif ke-4 dari 1 adalah bilangan kompleks *i* dan *–i*, sebab $\pm i \neq 1$, $(\pm i)^2 = -1 \neq 1$, $(\pm i)^3 = -i \neq 1$ tetapi $i^4 = 1$. Di sini −1 bukan akar primitif ke-4.

Sesungguhnya akar primitif ke-λ selalu bilangan kompleks. Tulisan di sini terpusat pada kasus λ adalah bilangan bulat prima dengan $2 < \lambda \leq 19$ dan ω adalah akar primitif ke-λ dari 1 yang merupakan akar ($\neq 1$) dari polinom berderajat $\lambda - 1$

$$f_\lambda(x) = \frac{x^\lambda - 1}{x - 1} = x^{\lambda-1} + ... + x + 1 \in \mathbf{Z}[x]. \qquad (1)$$

$f_\lambda(x)$, disebut **polinom siklotomik** ke-λ, memiliki sebanyak $\lambda - 1$ akar kompleks.

Di dalam Fraleigh [**Error! Reference source not found.**] (Theorem 23.15, hal. 215 – 216) dibuktikan bahwa polinom $f_\lambda(x)$ adalah polinom *irreducible* atas lapangan **Q** (dan **Z**). Di dalam lapangan siklotomik (*splitting field*) **Q(**ω**)**, lapangan terkecil yang memuat **Z**[ω] dan ω, $f_\lambda(x)$ tereduksi atas faktor-faktor linear yang memuat semua akar-akar dari $f_\lambda(x)$. Dari bentuk rasio $f_\lambda(x)$ di dalam (1), disimpulkan bahwa semua $\lambda - 1$ akar-akar dari $f_\lambda(x)$ memenuhi $x^\lambda - 1 = 0$, $x \neq 1$.

Karenaλprima, lapangan $\mathbf{Z}_\lambda^\times$ memiliki tepat sebanyak $\lambda - 1$ unsur. Menurut Lemma 6.1 [**Error! Reference source not found.**], ω adalah akar primitif dari $f_\lambda(x)$ jika dan hanya jika $x = \omega^2$, ..., $x = \omega^{\lambda-1}$ juga akar primitif padahal dari sifat tertutup grup perkalian, semua $\lambda - 1$ akar-akar primitif $x = \omega, x = \omega^2, ..., x = \omega^{\lambda-1}$ berada di dalam $\mathbf{Z}_\lambda^\times$. Fakta ini juga bisa diturunkan dari fakta bahwalapangan **Q(**ω**)** adalah perluasan Galois dari **Q**, jadi memuat semua akar-akar dari $f_\lambda(x)$. Ini berarti semua akar dari $f_\lambda(x)$ adalah akar primitif ke-λdari 1. Sebagai akibatnya, di dalam lapangan **Q(**ω**)** berlaku

$$f_\lambda(x) = (x - \omega)(x - \omega^2)...(x - \omega^{\lambda-1})$$

atau

$$f_\lambda(x) = \prod_{i=1}^{\lambda-1} (x - \omega^i). \qquad (2)$$

Perlu dicatat bahwa $f_\lambda(x)$ adalah polinom minimal dari setiap akar primitif ke-λdari 1. Karena semua koefisien dari $f_\lambda(x)$ adalah bilangan bulat, setiap akar primitif ke-λdari 1 adalah bilangan bulat aljabar (merupakan akar dari suatu polinom dengan koefisien-koefisien bulat).

Bentuk polinom $f_\lambda(x)$, polinom siklotomik ke-λ dengan $\lambda \in \mathbf{Z}$ prima, bisa diturunkan dari definisi umum polinom siklotomik ke-*n*, di mana $n \in 2, 3, 4, ...$ (*n* tidak harus prima) sebagai berikut

$$f_n(x) = \prod_{\substack{\omega \text{ akar primitif} \\ \text{ke-}n \text{ dari } 1}} (x - \omega).$$

Dengan kata lain

$$f_n(x) = \prod_{i \in \mathbf{Z}_n^\times} (x - \omega^i) \quad (4.3)$$

Pandang gelanggang

$$\mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\}.$$

Untuk nilai-nilai λ prima dengan $2 < \lambda \leq 19$ prima algoritma pembagian Euclid bisa diberlakukan di dalam $\mathbf{Z}[\omega]$. Sesungguhnya $\mathbf{Z}[\omega]$ yang dilengkapi fungsi Euclid

$$\delta: \mathbf{Z}[\omega] \rightarrow \mathbf{N}$$

dengan $\delta(\alpha) = \alpha\overline{\alpha}$ membentuk daerah Euclid (Lihat hal. 9, 75 dari [**Error! Reference source not found.**] atau Lemma 3.7 dari [7].

Sesungguhnya untuk setiap $\alpha, \beta \in \mathbf{Z}[\omega]$ berlaku $\delta(\alpha) < \delta(\alpha\beta)$ dan terdapat $\gamma, \rho \in \mathbf{Z}[\omega]$ sedemikian sehingga $\alpha = \gamma\beta + \rho$ dengan $0 \leq \delta(\rho) < \delta(\beta)$. Karena setiap daerah Euclid adalah sebuah PID (*Principal Ideal Domain*) dan setiap PID adalah sebuah UFD (*Unique Factorization Domain*), maka $\mathbf{Z}[\omega]$ merupakan UFD.

Jadi jika $2 < \lambda \leq 19$ prima, maka $\mathbf{Z}[\omega]$ merupakan daerah Euclid**,** jadijuga merupakan UFD (*Unique Factorization Domain*). Perlu dicatat bahwa bilangan prima berikutnya, $\lambda = 23$, dengan ω sebagai akar primitif ke-23, $\mathbf{Z}[\omega]$ bukan UFD.

Di dalam setiap daerah Euclid $\mathbf{Z}[\omega]$, konsep unit (unsur yang mempunyai invers) bisa diberlakukan. Lebih jauh, untuk setiap $\gamma \in \mathbf{Z}[\omega]$ yang bukan unit, bisa didefinisikan kelas kongruensi modulo γ berdasarkan relasi kongruensi berikut: dua unsur α, β berelasi modulo γ jika dan hanya jika unsur $\alpha - \beta$ adalah kelipatan γ (yaitu terdapat $\eta \in \mathbf{Z}[\omega]$ sedemikian sehingga $\alpha - \beta = \eta\gamma$).

Dua unsur $\alpha, \beta \in \mathbf{Z}[\omega]$ dikatakan **berasosiasi** satu sama lain jika terdapat unit μ sedemikian sehingga $\alpha = \mu\beta = \beta\mu$ (karena perkalian di dalam $\mathbf{Z}[\omega] \subseteq \mathbf{C}$ bersifat komutatif). Unsur $\gamma \in \mathbf{Z}[\omega]$ disebut unsur prima di dalam $\mathbf{Z}[\omega]$ jika $\gamma \mid \alpha\beta$ (γ membagi $\alpha\beta$) berakibat $\gamma \mid \alpha$atau $\gamma \mid \beta$.

Sebagai akibat algoritma pembagian Euclid, untuk setiap unsur $p \in \mathbf{Z}[\omega]$ yang bukan unit, ideal $p\mathbf{Z}[\omega]$ adalah ideal sejati dan gelanggang faktor $\mathbf{Z}[\omega]/p\mathbf{Z}[\omega]$ bukan gelanggang trivial. Pada khususnya jika $\pi \in \mathbf{Z}[\omega]$ adalah unsur prima (di dalam setiap PID, jadi di dalam setiap daerah Euclid), maka π identik *irreducible* sehingga ideal $<\pi>$ (notasi lain: $\pi\mathbf{Z}[\omega]$) maksimal. Sebagai akibatnya, gelangang faktor $\mathbf{Z}[\omega]/\pi\mathbf{Z}[\omega]$ adalah suatu lapangan. Banyak unsur di dalam lapangan ini adalah $\delta(\pi) = \pi\overline{\pi}$.

5. Simbol Residu Kubik

Misalkan ω adalah akar primitif ke-3 dari 1, $\alpha = a + ib \in \mathbf{Z}[\omega]$. Dengan fungsi Euclid

$$\delta: \mathbf{Z}[\omega] \rightarrow \mathbf{N}$$

di mana $\delta(\alpha) = \alpha\overline{\alpha} = a^2 + b^{2-} - ab$. Sifat multiplikatif dari δ berikut mudah dibuktikan:

$$(\forall \alpha, \beta \in \mathbf{Z}[\omega]).\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$$

Semua unit (unsur yang memiliki invers) di dalam $\mathbf{Z}[\omega]$ diperoleh dari fakta (Lemma 4.5 [**Error! Reference source not found.**]):

a. $\mu \in \mathbf{Z}[\omega]$ adalah unit jika dan hanya jika $\delta(\mu) = 1$
b. Himpunan semua unit di dalam $\mathbf{Z}[\omega]$ adalah $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Jika $\alpha \in \mathbf{Z}[\omega]$ memiliki norma $p = \delta(\alpha)$ yang merupakan unsur prima dalam $\mathbf{Z}$, maka αadalah unsur prima di dalam$\mathbf{Z}[\omega]$. Sebagai akibatnya, semua prima di dalam $\mathbf{Z}[\omega]$ bisa ditentukan berdasarkan pilihan bilangan prima p. Pertama kali ditentukan semua unsur prima π dengan norma $p = \delta(\pi)$.

a. Jika $p = 3$ maka $1 - \omega$ adalah unsur prima di dalam $\mathbf{Z}[\omega]$ dan $-\omega^2(1-\omega)^2 = 3$.
b. Jika $p \equiv 1 \bmod 3$ maka terdapat unsur prima π di dalam $\mathbf{Z}[\omega]$ dengan $p = \pi\bar{\pi}$, kedua unsur prima (di dalam $\mathbf{Z}[\omega]$) π dan $\bar{\pi}$ tidak berasosiasi.
c. Jika $p \equiv 2 \bmod 3$ maka p juga merupakan unsur prima di dalam $\mathbf{Z}[\omega]$.

Suatu unsur prima $\pi \in \mathbf{Z}[\omega]$ dengan norma $\delta(\pi)$ bukan bilangan prima selalu berasosiasi dengan unsur prima π' yang normanya adalah bilangan prima. Ini berarti terdapat unit μ dan bilangan prima π' sedemikian sehingga $\pi = \mu\pi'$. Jadi ideal $<\pi> = <\pi'>$adalah ideal maksimal dan sebagai akibatnya, gelanggang faktor $\mathbf{Z}[\omega]/<\pi>$atau $\mathbf{Z}[\omega]/<\pi'>$adalah lapangan.

Berikut adalah fakta-fakta yang berkaitan dengan unsur prima $\pi \in \mathbf{Z}[\omega]$ (Lemma 4.8 dan Corollary 4.9 dalam [**Error! Reference source not found.**]):

a. Banyak unsur di dalam lapangan $\mathbf{Z}[\omega]/<\pi>$adalah $N(\pi)$. Sebagai akibatnya, dari Teorema Kecil Fermat, untuk setiap $\alpha \in \mathbf{Z}[\omega]$ di mana π tidak membagi α berlaku

$$\alpha^{N(\pi)-1} \bmod \pi = 1.$$

(Perhatikan analoginya dengan pendefinisian simbol Legendre $\left(\frac{a}{p}\right)$ di mana p tidak membagi a).
b. Terdapat bilangan prima p sedemikian sehingga jika $N(\pi) = p$ dan
i. $p = 3$ atau $p \equiv 1 \bmod 3$, maka $N(\pi) = p$ dan $\mathbf{Z}/<p> \cong \mathbf{Z}[\omega]/<\pi>$**.**
ii. $p \equiv 2 \bmod 3$, maka $\mathbf{Z}/<p>$ adalah satu-satunya subgelanggang sejati berorder p dari $\mathbf{Z}[\omega]/<\pi>$ yang berorder $N(\pi) = p^2$.

Sebagai akibat dari butir *a*, untuk setiap $\alpha \in \mathbf{Z}[\omega]$ yang tidak habis dibagi π, unsur $s(\alpha) = \alpha^{(N(\pi)-1)/3} \bmod \pi$ adalah akar kubik (akar primitif ke-3) dari 1. Karena

$$x^3 - 1 \equiv (x-1)(x-\omega)(x-\omega^2) \bmod \pi$$

maka$s(\alpha) \equiv 1, \omega$ atau $\omega^2 \bmod \pi$. Dari sini, simbol Legendre (residu kuadratis) diperluas dengan mendefinisikan $s(\alpha)$ sebagai **simbol residu kubik** untuk $\alpha \in \mathbf{Z}[\omega]$ terhadap unsur prima $\pi \in \mathbf{Z}[\omega]$ dengan lambang $\left(\frac{\alpha}{\pi}\right)_3$, asalkan π tidak membagi α.Perhatikan, untuk setiap unsur $\alpha \in \mathbf{Z}[\omega]$ yang tidak habis dibagi π berlaku

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv 1, \omega \text{ atau } \omega^2 \bmod \pi$$

atau

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \bmod \pi.$$

Dari bentuk perluasan simbol residu kudratis Legendre $\left(\frac{a}{p}\right)$ dengan *p* prima di dalam **Z** ke simbol $\left(\frac{\alpha}{\pi}\right)_3$ dengan π unsur prima di dalam **Z**[ω], seperti halnya perluasan simbol residu kuadratis Legendre $\left(\frac{a}{p}\right)$ ke simbol residu kuadratis Jacobi $\left(\frac{a}{b}\right)$, di mana *b* tidak harus bilangan prima, simbol residu kubik $\left(\frac{\alpha}{\pi}\right)_3$ bisa diperluas ke simbol residu kubik $\left(\frac{\alpha}{\beta}\right)_3$ untuk sembarang pasangan unsur $\alpha, \beta \in$**Z**[ω] di mana β tidak harus prima di dalam **Z**[ω].

Seperti halnya perluasan $\left(\frac{a}{p}\right)$ ke $\left(\frac{a}{b}\right)$ di dalam **Z** bisa diberlakukan karena **Z** adalah UFD sehingga bilangan bulat *b* bisa diuraikan secara tunggal atas faktor-faktornya, perluasan $\left(\frac{\alpha}{\pi}\right)_3$ ke $\left(\frac{\alpha}{\beta}\right)_3$ di dalam **Z**[ω] bisa diberlakukan karena **Z**[ω] adalah UFD sehingga unsur $\beta \in$**Z**[ω]bisa diuraikan secara tunggal atas faktor-faktornya.

Salah satu algoritma efisien untuk mencari unsur prima $\pi \in$**Z**[ω] dengan norm $\delta(\pi) = p \in$**Z** prima, bisa dijumpai di dalam [9]. Contoh penggunaan algoritma ini bisa diuraikan secara singkat sebagai berikut.Misalnya dari bilangan prima $p \equiv 1 \pmod 3$ yang diberikan, lebih dulu ditentukan nilai *s* dan *t* yang memenuhi

$$p = s^2 + 3t^2 = (s + t)^2 - 2t(s + t) + 4t^2.$$

Agar $p \equiv 1 \pmod 3$ dipenuhi, kesamaan $s^2 = 1$ dan $t^2 \in$**Z** harus dipenuhi. Dengan memilih $a = s + t$ dan $b = 2t$,diperoleh$p = a^2 - ab + b^2$. Jadi jika $\pi = a + b\omega \in$**Z**[ω], maka$\delta(\pi) = p$.

Untuk menentukan nilai simbol residu kuadratis $\left(\frac{\alpha}{\beta}\right)_3$ kembali pustaka [9] memberikan sebuah algoritma yang pada dasarnya melakukan iterasi perhitungan nilai $\left(\frac{\alpha}{\gamma}\right)_3$ dan *g* yang memenuhi $\left(\frac{\alpha}{\beta}\right)_3 = \omega^g \left(\frac{\alpha}{\gamma}\right)_3$ dan $\delta(\gamma) < \delta(\beta)$. Iterasi berakhir ketika diperoleh simbol residu berbentuk $\left(\frac{\pm 1}{\delta}\right)_3 = 1$.

Lapangan siklotomik menjadi dasar dari skema kriptografi publik, seperti yang disajikan secara kronologis dalam [9], [7], [8] dan [**Error! Reference source not found.**]. Di dalam [**Error! Reference source not found.**] misalnya, penerapan kriptografi untuk kasus $\lambda = 2$, diawali dengan menentukan nilai simbol Jacobi $\left(\frac{N-1}{pq}\right)$ yang berbasis residu kuadratis, sedangkan dalam kasus $\lambda = 3$, diawali dengan mementukan nilai simbol residu kubik lebih dulu.

6. Penutup

Dari diskusi pada bagian sebelumnya diturunkan bahwa lapangan siklotomik ke-2 tidak lain adalah **Q** dan akar primitif ke-2 adalah −1. Jadi daerah faktorisasi tunggal terkecil yang memuat −1 adalah **Z**. Tetapi mulai dari $\lambda = 3$, lapangan siklotomik ke-3 **Q(**ω**)** memuat daerah Euclid **Z**[ω] yang juga merupakan daerah faktorisasi tunggal. Unsur prima $\pi \in$**Z**[ω] menentukan lapangan **Z**[ω]/<π> dan simbol residu kubik $\left(\frac{\alpha}{\pi}\right)_3$, untuk setiap setiap $\alpha \in$**Z**[ω] yang tidak habis dibagi π.

Fakta di atas sebenarnya berlaku untuk sembarang ω adalah akar primitif ke-λ dengan $0 \leq \lambda \leq 19$ dan λ prima. Daerah Euclid $\mathbf{Z}[\omega]$ bersama lapangan siklotomik $\mathbf{Z}[\omega]/<\pi>$memiliki potensi dalam rancangan konstruksi kriptografi publik.

Daftar Pustaka

[1] Cox D.A., 1989. *Primes of the Forms* $x^2 + ny^2$. John Wiley & Sons, Toronto, Canada.

[2] Despotovic Z.A Public-Key Cryptosystem Using Cyclotomic Fields. *EPFL DSC Graduate School Project Report.*

[3] FraleighJ.B., 2002. *A First Course in Abstract Algebra*, Edisi 7. Addison Wesley.

[1] IrelandK. dan Rosen M., 1990.*A Classical Introduction to Modern Theory of Numbers*, Edisi 2. Springer-Verlag, New York.

[2] Menezes A., van Oorschot P., Vanstone S., 1996. *Handbook of Applied Cryptography*. CRC Press.

[6] MilneJ.S., 2009. *Algebraic Number Theory. Versi 3.02*. URL: www.jmilne.org/math/ [Diakses pada tanggal 3 Maret 2010]

[7] Scheidler R.1993.*Applications of Algebraic Number Theory to Cryptography*.*Disertasi*.Department of Computer Science, University of Manitoba, Canada.

[3] Scheidler R. dan Williams H.C., 1995. A Public-Key Cryptosystem Utilizing Cyclotomic Fields.*Designs, Codes and Cryptography*,**7** (1 - 2): hal. 153-174.

[4] Williams H.C., 1986.An M^3Public-Key Encryption Scheme. Advances in Cryptology - CRYPTO ’85 (*Proceedings*), pp. 358 – 36. Springer, Berlin.